

《现代交换原理》实验报告

实验名称 拨打 SIP 电话

班 级 2017211307

学 号 2017211335 2017211336 2017211337

姓 名 王 兴 宇 刘 凯 鑫 刘 兴 贤

指导教师 丁 玉 荣

一、实验目的

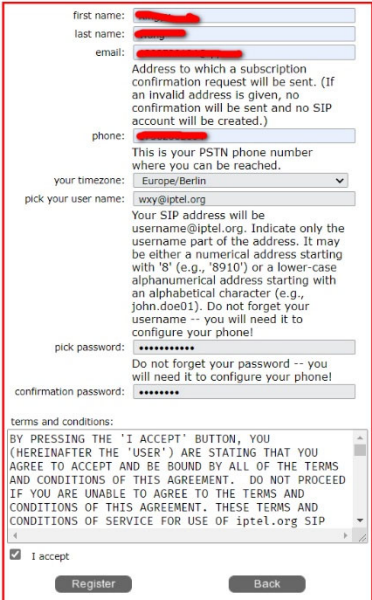
本实验需要实验者结合课堂所讲的 SIP 信令工作流程,对软电话呼叫的信令进行抓包分析,理解 VoIP 呼叫中会话信令、媒体协商信令的作用,从而加深对 VoIP 的理解。

二、实验内容和实验步骤

1. 下载软件并注册 SIP 账号

首先我们先注册一个 SIP 账号

进入 <https://serweb.iptel.org/user/reg/index.php>

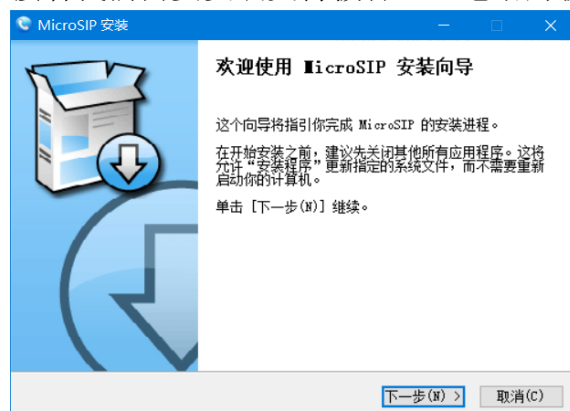


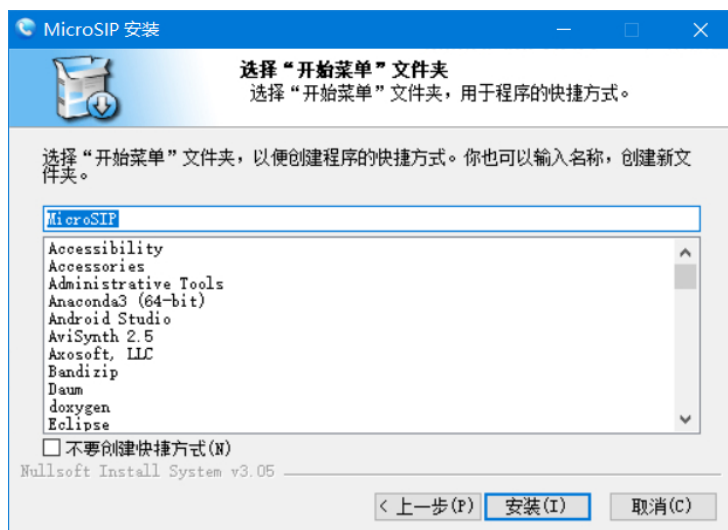
first name: [redacted]
last name: [redacted]
email: [redacted]
Address to which a subscription confirmation request will be sent. (If an invalid address is given, no confirmation will be sent and no SIP account will be created.)
phone: [redacted]
This is your PSTN phone number where you can be reached.
your timezone: Europe/Berlin
pick your user name: wxy@iptel.org
Your SIP address will be username@iptel.org. Indicate only the username part of the address. It may be either a numerical address starting with '8' (e.g., '8910') or a lower-case alphanumerical address starting with an alphabetical character (e.g., john.doe01). Do not forget your username -- you will need it to configure your phone!
pick password: [redacted]
Do not forget your password -- you will need it to configure your phone!
confirmation password: [redacted]
terms and conditions:
BY PRESSING THE 'I ACCEPT' BUTTON, YOU (HEREINAFTER THE 'USER') ARE STATING THAT YOU AGREE TO ACCEPT AND BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. DO NOT PROCEED IF YOU ARE UNABLE TO AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. THESE TERMS AND CONDITIONS OF SERVICE FOR USE OF iptel.org SIP
☒ I accept
Register Back

本实验中,本组三名成员都注册了 SIP 账号。分别是:

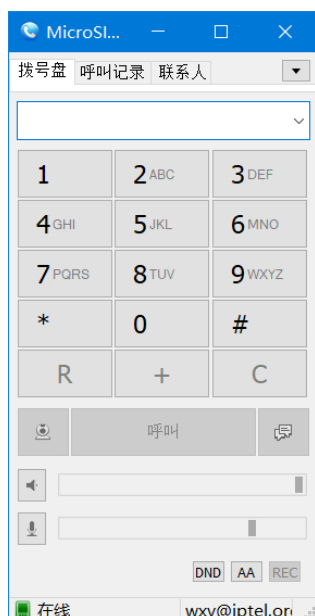
wxy@iptel.org axin@iptel.org liuxingxian@iptel.org

接着我们需要安装支持拨打 SIP 电话的软件,这里我们使用的是 MicroSIP。





显示安装成功后，界面如下：



接着我们需要登录账号并配置好软件。

帐号

帐号名 王兴宇

SIP 服务器 iptel.org

SIP 代理

用户 * wxxy@iptel.org

域名 * wxxy@iptel.org

登录名 wxxy

密码
[显示密码](#)

显示名称 wxxy

语音信箱号码

拨号前缀

Dial Plan

☐ Hide Caller ID

加密媒体 禁用

透传 自动 (UDP & TCP)

公共地址 自动

刷新注册 300 保持在线 15

☐ 发布状态

☐ 允许 IP 重写

☐ ICE

☐ 禁用会话计时器

保存 取消

输入想要拨打的对方的 SIP 地址，点击呼叫即可拨号，可以听到回铃音。说明软件配置完成，可以进行拨号抓包实验。

MicroSI...

拨号盘 呼叫记录 联系人

axin@iptel.org

1 2 ABC 3 DEF

4 GHI 5 JKL 6 MNO

7 PQRS 8 TUV 9 WXYZ

* 0 #

< + C

呼叫

音量

麦克风

DND AA REC

在线 wxxy@iptel.org

2. 拨打电话并抓包分析

SIP 电话在拨出后，具体情况是不可预测的，其状态为下列之一：

- 被叫不接，持续响铃
- 被叫将其挂断
- 主叫将其挂断
- 接通后任意一方挂断
- 被叫正在忙碌（可能正在与其他人通话）

因此我们将分别讨论以上 5 种情况。

2.1 被叫不接，持续响铃

情景：主叫(wxy)拨打电话给被叫(axin)，被叫超时未接听

流程分析：

PPT 中给出的流程图如下（但实验中此处出现了不同）：



(1) 用户摘机发起一路呼叫，终端代理 A 向该区域代理服务器发起 Invite 请求；

(2) 代理服务器向被叫终端代理 B 传送 Invite 请求。

(3) 代理服务器向终端代理 A 发送呼叫处理中的应答信息：100 Trying。

(4) 终端代理 B 向代理服务器送呼叫处理中的应答信息：100 Trying。

(5) 被叫用户振铃，终端代理 B 向代理服务器送 180Ring 响应。

(6) 代理服务器向终端代理 A 转发该响应信息。

(7) 被叫久振铃无应答，终端代理 B 判断超时后向代理服务器送 408 Request Timeout 消息放弃该呼叫。

(8) 代理服务器收到 408 Request Timeout 消息后，转发该消息给终端代理 A。

(9) 代理服务器回送 ACK 确认给终端代理 B。

(10) 终端代理 A 向代理服务器回送 ACK 确认。

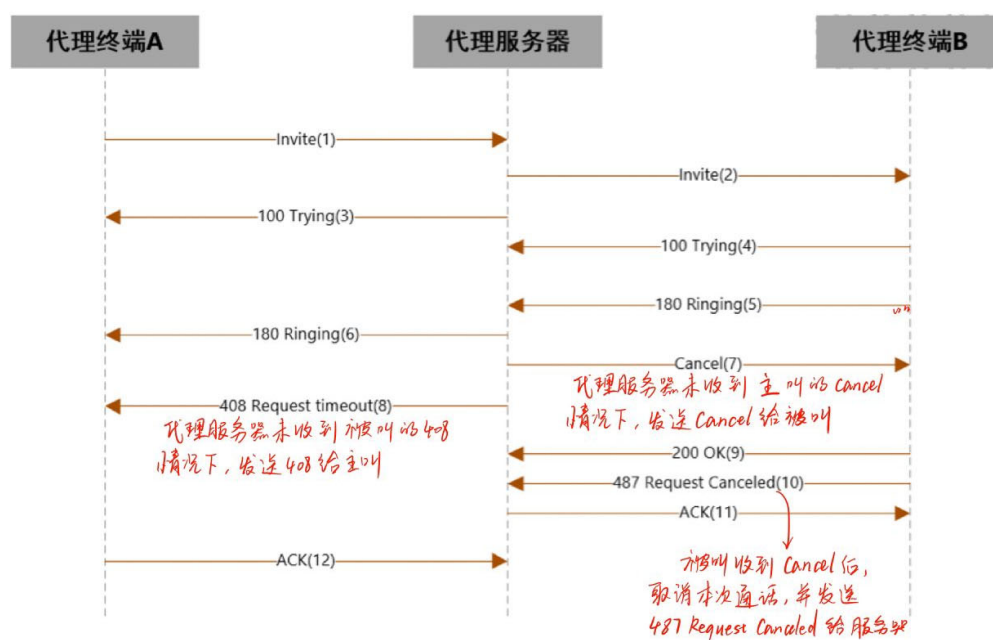
Wireshark 抓包分析：

Source	Destination	Protocol	Length	Info
192.168.0.106	212.79.111.155	SIP	559	Request: REGISTER sip:iptel.org (1 binding)
212.79.111.155	192.168.0.106	SIP	459	Status: 200 OK (1 binding)
192.168.0.106	212.79.111.155	SIP	559	Request: REGISTER sip:iptel.org (1 binding)
212.79.111.155	192.168.0.106	SIP	459	Status: 200 OK (1 binding)
192.168.0.106	212.79.111.155	SIP/SDP	1000	Request: INVITE sip:axin@iptel.org (1 binding)
212.79.111.155	192.168.0.106	SIP	364	Status: 100 Trying
212.79.111.155	192.168.0.106	SIP	772	Status: 407 Proxy Authentication Required
192.168.0.106	212.79.111.155	SIP	402	Request: ACK sip:axin@iptel.org (1 binding)
192.168.0.106	212.79.111.155	SIP/SDP	1176	Request: INVITE sip:axin@iptel.org (1 binding)
212.79.111.155	192.168.0.106	SIP	411	Status: 100 Trying
212.79.111.155	192.168.0.106	SIP	665	Status: 180 Ringing
192.168.0.106	212.79.111.155	SIP	559	Request: REGISTER sip:iptel.org (1 binding)
212.79.111.155	192.168.0.106	SIP	459	Status: 200 OK (1 binding)
212.79.111.155	192.168.0.106	SIP	665	Status: 180 Ringing
192.168.0.106	212.79.111.155	SIP	559	Request: REGISTER sip:iptel.org (1 binding)
212.79.111.155	192.168.0.106	SIP	459	Status: 200 OK (1 binding)
212.79.111.155	192.168.0.106	SIP	671	Status: 408 Request Timeout
192.168.0.106	212.79.111.155	SIP	402	Request: ACK sip:axin@iptel.org (1 binding)
192.168.0.106	212.79.111.155	SIP	559	Request: REGISTER sip:iptel.org (1 binding)
212.79.111.155	192.168.0.106	SIP	459	Status: 200 OK (1 binding)
192.168.0.106	212.79.111.155	SIP	559	Request: REGISTER sip:iptel.org (1 binding)
212.79.111.155	192.168.0.106	SIP	781	Status: 401 Unauthorized

> Frame 22218: 1176 bytes on wire (9408 bits), 1176 bytes captured (9408 bits) on interface \Device\NPF{...} Ethernet II, Src: HonHaiPr_7f:d4:d9 (f8:da:0c:7f:d4:d9), Dst: Tp-LinkT_3c:b8:35 (60:3a:7c:3c:b8:35) Internet Protocol Version 4, Src: 192.168.0.106, Dst: 212.79.111.155 User Datagram Protocol, Src Port: 5060, Dst Port: 5060 Session Initiation Protocol (INVITE)

实际流程和 ppt 不完全相同，这里给出抓包得到的流程图：

被叫无应答：



可以看到，与 PPT 中不同的是，并不是由被叫的终端代理发出 408timeout，而是由主叫在定时器超时后，发出 cancel 包，然后代理服务器返回 408timeout。被叫收到 cancel 后，取消本次通话，并发送 487cancel 给代理服务器通知自己已经取消通话。

这里与 PPT 在实现机制上还是稍有不同，但也相当合理。猜测可能是不同软件的实现方式不同。可作为本实验与预想结果不同的一点加以讨论。

2.2 被叫将其挂断

情景：主叫(liuixngxian)拨打电话给被叫(axin)，被叫超时未接听
流程分析：

PPT 中给出的流程图如下



接着我们使用 wireshark 进行抓包：
主叫抓包：

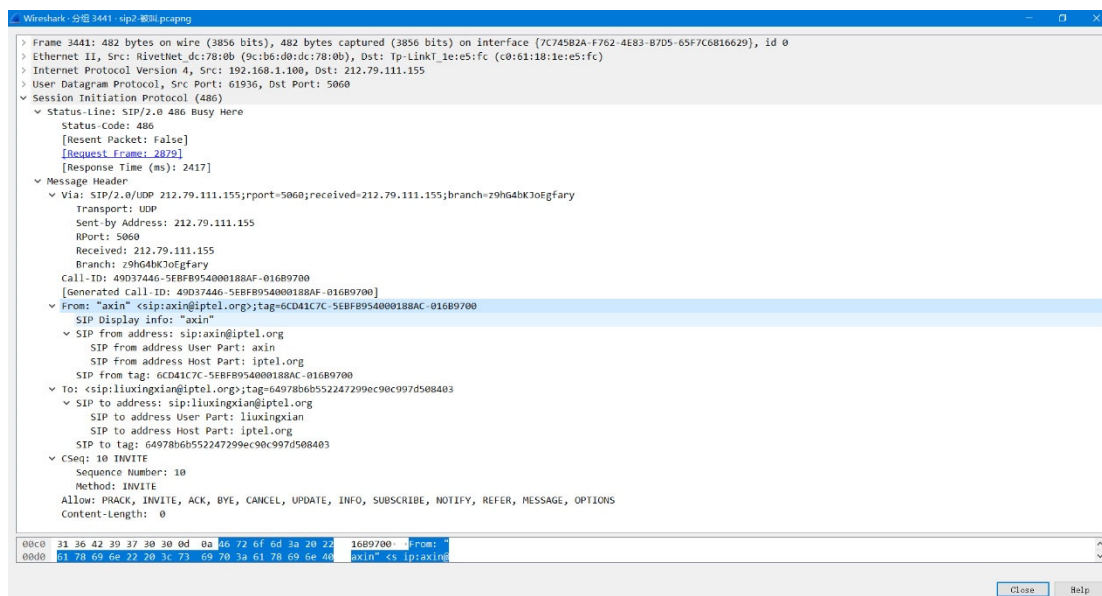
No.	Time	Source	Destination	Protocol	Length	Info
2285	8.851685	192.168.2.120	212.79.111.155	SIP	562	Request: REGISTER sip:iptel.org (1 binding)
2339	9.049994	212.79.111.155	192.168.2.120	SIP	460	Status: 200 OK (1 binding)
3343	12.730210	192.168.2.120	212.79.111.155	SIP/SDP	1014	Request: INVITE sip:liuxingxian@iptel.org
3380	12.928289	212.79.111.155	192.168.2.120	SIP	370	Status: 100 Trying
3381	12.929220	212.79.111.155	192.168.2.120	SIP	792	Status: 407 Proxy Authentication Required
3382	12.929505	192.168.2.120	212.79.111.155	SIP	417	Request: ACK sip:liuxingxian@iptel.org
3383	12.929744	192.168.2.120	212.79.111.155	SIP/SDP	1198	Request: INVITE sip:liuxingxian@iptel.org
3429	13.123817	212.79.111.155	192.168.2.120	SIP	417	Status: 100 Trying
3622	13.785432	212.79.111.155	192.168.2.120	SIP	671	Status: 180 Ringing
3994	15.726826	212.79.111.155	192.168.2.120	SIP	593	Status: 486 Busy Here
3995	15.727134	192.168.2.120	212.79.111.155	SIP	417	Request: ACK sip:liuxingxian@iptel.org
14754	64.349467	192.168.2.120	212.79.111.155	SIP	562	Request: REGISTER sip:iptel.org (1 binding)
14773	64.544914	212.79.111.155	192.168.2.120	SIP	460	Status: 200 OK (1 binding)

被叫抓包：

No.	Time	Source	Destination	Protocol	Length	Info
539	2.688213	192.168.1.100	212.79.111.155	SIP	568	Request: REGISTER sip:iptel.org (1 binding)
578	2.853896	212.79.111.155	192.168.1.100	SIP	468	Status: 200 OK (1 binding)
2879	11.388008	212.79.111.155	192.168.1.100	SIP/SDP	1182	Request: INVITE sip:liuxingxian@125.47.235.1:6371;ob
2889	11.417591	192.168.1.100	212.79.111.155	SIP	344	Status: 100 Trying
2890	11.418201	192.168.1.100	212.79.111.155	SIP	529	Status: 180 Ringing
3046	11.863315	212.79.111.155	192.168.1.100	SIP/SDP	1182	Request: INVITE sip:liuxingxian@125.47.235.1:6371;ob
3047	11.863861	192.168.1.100	212.79.111.155	SIP	529	Status: 180 Ringing
3441	13.805445	192.168.1.100	212.79.111.155	SIP	482	Status: 486 Busy Here
3463	13.984840	212.79.111.155	192.168.1.100	SIP	378	Request: ACK sip:liuxingxian@125.47.235.1:6371;ob
13153	57.855777	192.168.1.100	212.79.111.155	SIP	568	Request: REGISTER sip:iptel.org (1 binding)
13177	58.021246	212.79.111.155	192.168.1.100	SIP	468	Status: 200 OK (1 binding)

可以发现主叫和被叫在通话前甚至通话中都有 REGISTER 过程，这个是要保证与 SIP 代理服务器连接，大约每隔 55s 发送一次。当主叫 liuxingxian@iptel.org 拨打电话后，首先是给代理服务器发送 INVITE 包，代理服务器转发给被叫 axin@iptel.org，可以看到被叫收到了 INVITE 包。然后被叫会送 100 Trying 包，在第一个图中可以看出，主叫成功收到了来自被叫 axin@iptel.org 的 100 Trying 包，此时被叫会送 180 Ringing 包，主叫受到 180 Ringing 包后回铃音响起。此时如果被叫挂断电话，就会向代理服务器发送 486 Busy here 包，代理服务器将这个包发送给主叫，主叫受到 486 Busy here 包，得知被叫挂断了电话，此时停止回铃音，发送 ACK 给被叫，被叫正常收到了 ACK，整个被叫忙呼叫过程结束。

下面是 486 Busy here 包的详细内容，可以看出确实是由被叫 axin@iptel.org 发送给了主叫 liuxingxian@iptel.org，符合 SIP 流程预期。



2.3 主叫将其挂断

情景：主叫(liuixngxian)拨打电话给被叫(wxy)，被叫未接听，主叫主动释放。

流程分析：

PPT 中给出的流程图如下



接着我们使用 wireshark 进行抓包来验证上述流程。

主叫：

No.	Time	Source	Destination	Protocol	Length	Info
2292	14.174722	192.168.1.100	212.79.111.155	SIP/SDP	1006	Request: INVITE sip:wxy@iptel.org
2334	14.340641	212.79.111.155	192.168.1.100	SIP	363	Status: 100 Trying
2335	14.342568	212.79.111.155	192.168.1.100	SIP	770	Status: 407 Proxy Authentication Required
2336	14.343042	192.168.1.100	212.79.111.155	SIP	402	Request: ACK sip:wxy@iptel.org
2337	14.343800	192.168.1.100	212.79.111.155	SIP/SDP	1189	Request: INVITE sip:wxy@iptel.org
2384	14.510760	212.79.111.155	192.168.1.100	SIP	410	Status: 100 Trying
2440	14.688245	212.79.111.155	192.168.1.100	SIP	664	Status: 180 Ringing
3175	18.470826	192.168.1.100	212.79.111.155	SIP	399	Request: CANCEL sip:wxy@iptel.org
3201	18.672710	212.79.111.155	192.168.1.100	SIP	445	Status: 200 OK
3202	18.672714	212.79.111.155	192.168.1.100	SIP	461	Status: 487 Request terminated
3207	18.673655	192.168.1.100	212.79.111.155	SIP	402	Request: ACK sip:wxy@iptel.org
5794	30.453797	192.168.1.100	212.79.111.155	SIP	568	Request: REGISTER sip:iptel.org (1 binding)
5858	30.640229	212.79.111.155	192.168.1.100	SIP	785	Status: 401 Unauthorized
5859	30.640757	192.168.1.100	212.79.111.155	SIP	741	Request: REGISTER sip:iptel.org (1 binding)
5902	30.810692	212.79.111.155	192.168.1.100	SIP	717	Status: 200 OK (1 binding)

被叫：

No.	Time	Source	Destination	Protocol	Length	Info
2186	13.101668	212.79.111.155	192.168.0.106	SIP/SDP	1166	Request: INVITE sip:wxy@10.179.151.48:52029;ob
2188	13.112248	192.168.0.106	212.79.111.155	SIP	336	Status: 100 Trying
2189	13.112661	192.168.0.106	212.79.111.155	SIP	516	Status: 180 Ringing
3034	17.234800	212.79.111.155	192.168.0.106	SIP	782	Request: CANCEL sip:wxy@10.179.151.48:52029;ob
3035	17.235020	192.168.0.106	212.79.111.155	SIP	369	Status: 200 OK
3036	17.235085	192.168.0.106	212.79.111.155	SIP	483	Status: 487 Request Terminated
3113	17.735213	192.168.0.106	212.79.111.155	SIP	483	Status: 487 Request Terminated
3134	17.897667	212.79.111.155	192.168.0.106	SIP	364	Request: ACK sip:wxy@10.179.151.48:52029;ob
5834	30.768508	192.168.0.106	212.79.111.155	SIP	559	Request: REGISTER sip:iptel.org (1 binding)
5856	30.940829	212.79.111.155	192.168.0.106	SIP	459	Status: 200 OK (1 binding)

可以看到，首先会由主叫发出一个 Invite 包，向代理服务器发送一个会话邀请，在该包中指明目的地址，将会经由代理服务器转发到目的终端。然后收到一个 100trying，该 Invite 包会经由代理服务器发给被叫终端。同样的被叫也会向代理服务器回一个 100trying。

值得注意的是，每次主叫拨出后，都会进行两次 Invite 包的发送，然而被叫端只听到一个包。同时两次 Invite 包中间还会由代理服务器返回一个 407（经多次实验总是这样），经查阅资料，该包用于鉴权，二次 Invite 鉴权机制将会在 2.4 中进行解释。包内容的解析也会放在 2.4 通话过程中。

接受到会话邀请后，被叫终端会向主叫返回一个回铃音（当然，这需要经由代理服务器传输）。

然后主叫端在等待一段时间后，发现对方并未接听，因此手动挂机。此时，由主叫向目的端发送一个 cancel 包，代理服务器与目的终端接收到后都会返回一个 200OK。

最后会由被叫返回一个 487 request canceled 包通知主叫终端，自己已经释放了这个半开连接。会话成功终止。

可以看到，主叫主动挂断是与预想的流程完全一致的。

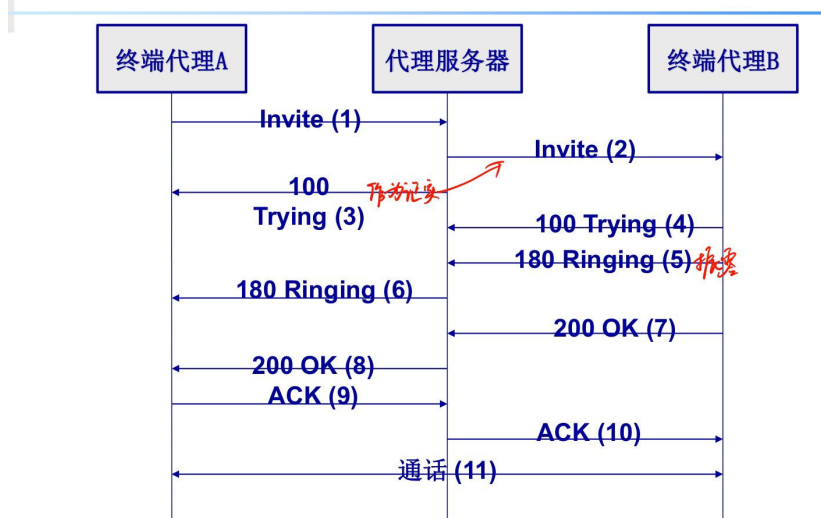
2.4 接通后任意一方挂断

情景：主叫呼叫被叫，接通电话一段时间后，主叫或被叫挂机

流程图如下：

呼叫建立：

3)、基本呼叫建立过程



(1)用户摘机发起一路呼叫,终端代理 A 向该区域的代理服务器发起 Invite 请求;

(2)代理服务器通过认证/计费中心确认用户认证已通过后,检查请求消息中的 Via 头域中是否已包含其地址。若已包含,说明发生环回,返回指示错误的应答;若没有问题,代理服务器在请求消息的 Via 头域插入自身地址,并向 Invite 消息的 To 域所指示的被叫终端代理 B 传送 Invite 请求。

(3)代理服务器向终端代理 A 发送呼叫处理中的应答信息: 100 Trying。

(4)终端代理 B 向代理服务器送呼叫处理中的应答信息: 100 Trying。

(5)终端代理 B 指示被叫用户振铃,用户振铃后向代理服务器发送 180 Ringing 振铃信息。

(6)代理服务器向终端代理 A 转发被叫用户振铃信息。

(7)被叫用户摘机,终端代理 B 向代理服务器返回表示连接成功的应答 200 OK

(8)代理服务器向终端代理 A 转发该成功指示 200 OK

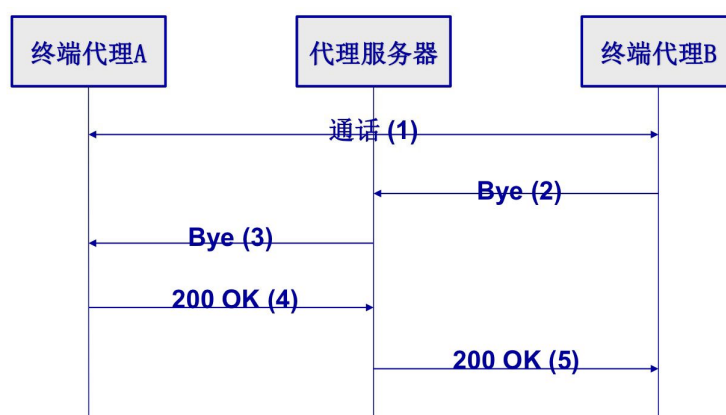
(9)终端代理 A 收到信息后,向代理服务器发 ACK 信息进行确认

(10)代理服务器将 ACK 确认消息转发给终端代理 B。

(11)主被叫用户之间建立通信连接,开始通话。

呼叫释放:

4)、正常呼叫释放过程 (Bye 可由 A 或 B 发起)



(1) 正常呼叫

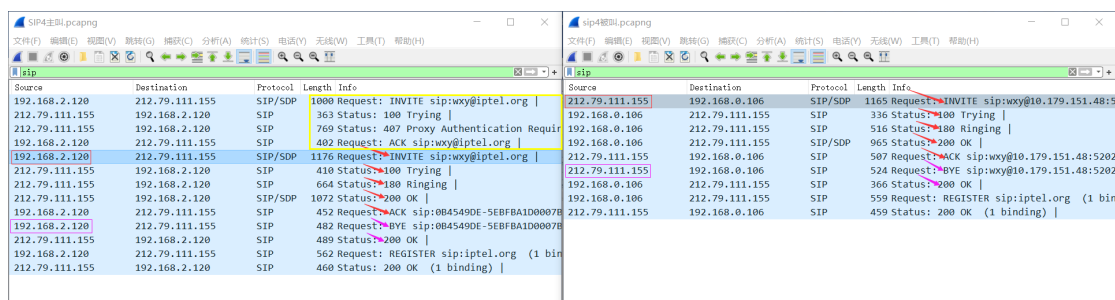
(2) 用户通话结束后,被叫用户挂机,终端代理 B 向代理服务器发送 Bye 消息。

(3)代理服务器转发 Bye 消息至终端代理 A,同时向认证、计费中心发送用户通话的详细信息,请求计费。

(4)主叫用户挂机后,终端代理 A 向代理服务器发送确认挂断响应信息 200 OK。

(5)代理服务器转发响应信息 200 OK。

下面我们使用 Wireshark 抓取具体的包来证明上述过程。
Wireshark 抓包分析：



Source	Destination	Protocol	Length	Info
192.168.2.120	212.79.111.155	SIP/SDP	1000	Request: INVITE sip:wxy@iptel.org
212.79.111.155	192.168.2.120	SIP	363	Status: 100 Trying
212.79.111.155	192.168.2.120	SIP	769	Status: 407 Proxy Authentication Required
192.168.2.120	212.79.111.155	SIP	402	Request: ACK sip:wxy@iptel.org
192.168.2.120	212.79.111.155	SIP/SDP	1176	Request: INVITE sip:wxy@iptel.org
212.79.111.155	192.168.2.120	SIP	410	Status: 100 Trying
212.79.111.155	192.168.2.120	SIP	664	Status: 180 Ringing
212.79.111.155	192.168.2.120	SIP/SDP	1072	Status: 200 OK
192.168.2.120	212.79.111.155	SIP	452	Request: ACK sip:004549DE-5EBFBA1D0007B1D8-C5066700
192.168.2.120	212.79.111.155	SIP	482	Request: BYE sip:004549DE-5EBFBA1D0007B1D8-C5066700
212.79.111.155	192.168.2.120	SIP	489	Status: 200 OK
192.168.2.120	212.79.111.155	SIP	562	Request: REGISTER sip:iptel.org (1 binding)
212.79.111.155	192.168.2.120	SIP	460	Status: 200 OK (1 binding)

抓包过程中，正如我们刚刚说明的那样，每一次会话建立都会发送两次 Invite 包，同时中间会收到一次代理服务器发送的 407 Proxy Authentication Required。

下面我们将试图解释一下鉴权过程：

该包事实上是用于鉴权，是为了验证主叫的身份。该鉴权的基本流程为：

- 用户代理客户端（UAC）将 SIP 消息发送到用户代理服务器（UAS）
- UAS 以 4xx 质询回应
- UAC 使用 4xx 质询响应中的数据来加密其身份凭证
- UAC 使用加密的凭证重新发送 SIP 消息

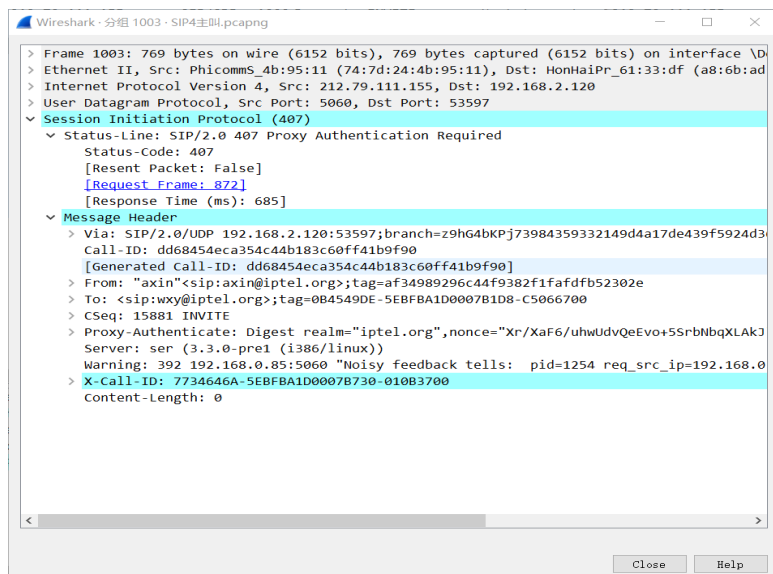
在 Proxy-Authenticate 标头中，可以看到一个 Nonce 参数。Nonce 代表“一次编号”，是在密码通信中仅使用一次的任意数字。Nonce 的接收者将使用它来作为加密凭据，加密方法是单向不对称的 SHA2 加密算法（查看了官方文档，发现之前是 MD5 校验，现在已普遍改为 SHA2）。

加密后该加密的密码放入 Proxy-Authentication 标头的响应参数中，来进行鉴权。该鉴权方法被普遍用于 HTTP 与 HTTPS 协议。

解释如下：

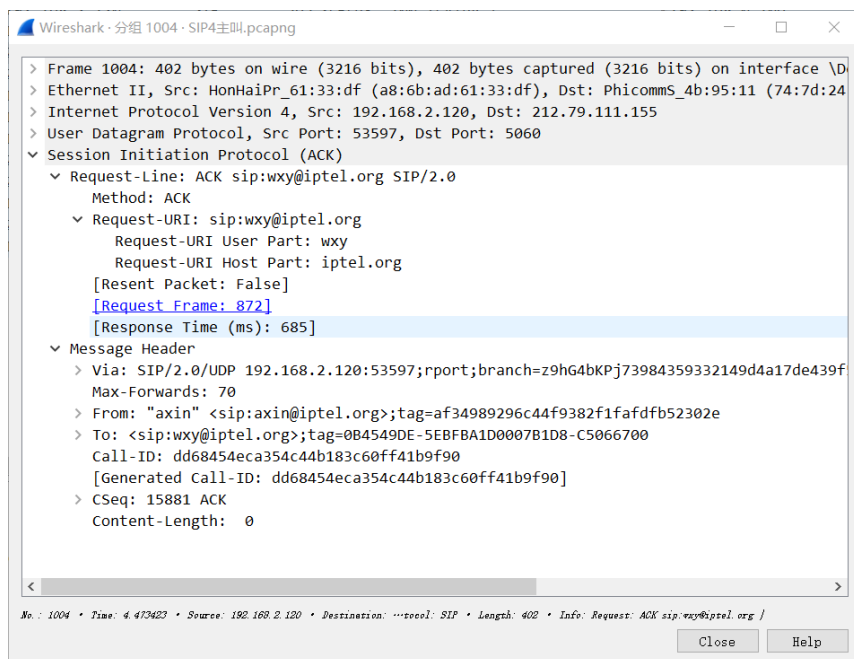
407 Proxy Authentication Required，这个返回码和 401 (Unauthorized) 很类似，但是标志了客户端应当首先在 proxy 上通过认证。这个返回码用于应用程序访问通讯网关（比如，电话网关），而很少用于被叫方要求认证。

407 Proxy Authentication Required 包内容如下：

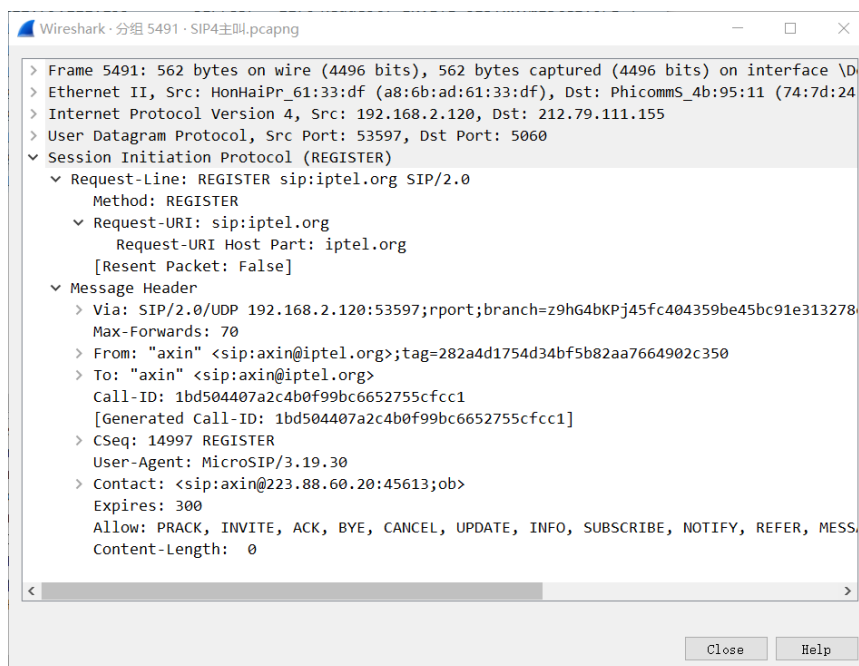


```
> Frame 1003: 769 bytes on wire (6152 bits), 769 bytes captured (6152 bits) on interface \Device\NPF{...}
> Ethernet II, Src: Phicomms_4b:95:11 (74:7d:24:4b:95:11), Dst: HonHaiPr_61:33:df (a8:6b:ad:61:33:df)
> Internet Protocol Version 4, Src: 212.79.111.155, Dst: 192.168.2.120
> User Datagram Protocol, Src Port: 5060, Dst Port: 53597
< Session Initiation Protocol (407)
  Status-Line: SIP/2.0 407 Proxy Authentication Required
    Status-Code: 407
    [Resent Packet: False]
    [Request Frame: 872]
    [Response Time (ms): 685]
  Message Header
    > Via: SIP/2.0/UDP 192.168.2.120:53597;branch=z9hG4bKpj73984359332149d4a17de439f5924d3;Call-ID: dd68454eca354c44b183c60ff41b9f90
    > Call-ID: dd68454eca354c44b183c60ff41b9f90
    > From: "axin"<sip:axin@iptel.org>;tag=af34989296c44f9382f1fafdfb52302e
    > To: <sip:wxy@iptel.org>;tag=0B4549DE-5EBFBA1D0007B1D8-C5066700
    > CSeq: 15881 INVITE
    > Proxy-Authenticate: Digest realm="iptel.org",nonce="Xr/XaF6/uhwUdvQeEvo+5SrBNbqXLakJServer: ser (3.3.0-pre1 (i386/linux))
    > Warning: 392 192.168.0.85:5060 "Noisy feedback tells: pid=1254 req_src_ip=192.168.0.85"
    > X-Call-ID: 7734646A-5EBFBA1D0007B730-010B3700
    Content-Length: 0
```

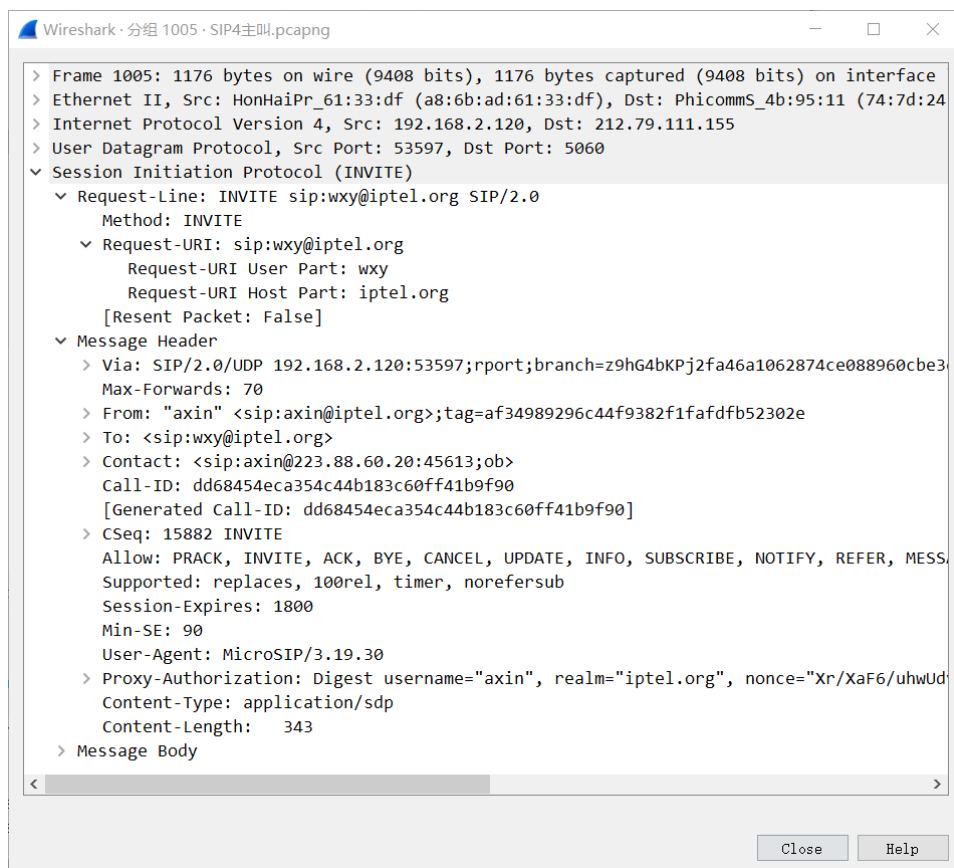
主叫针对 407 鉴权，发送给代理服务器的 ACK 包内容如下：



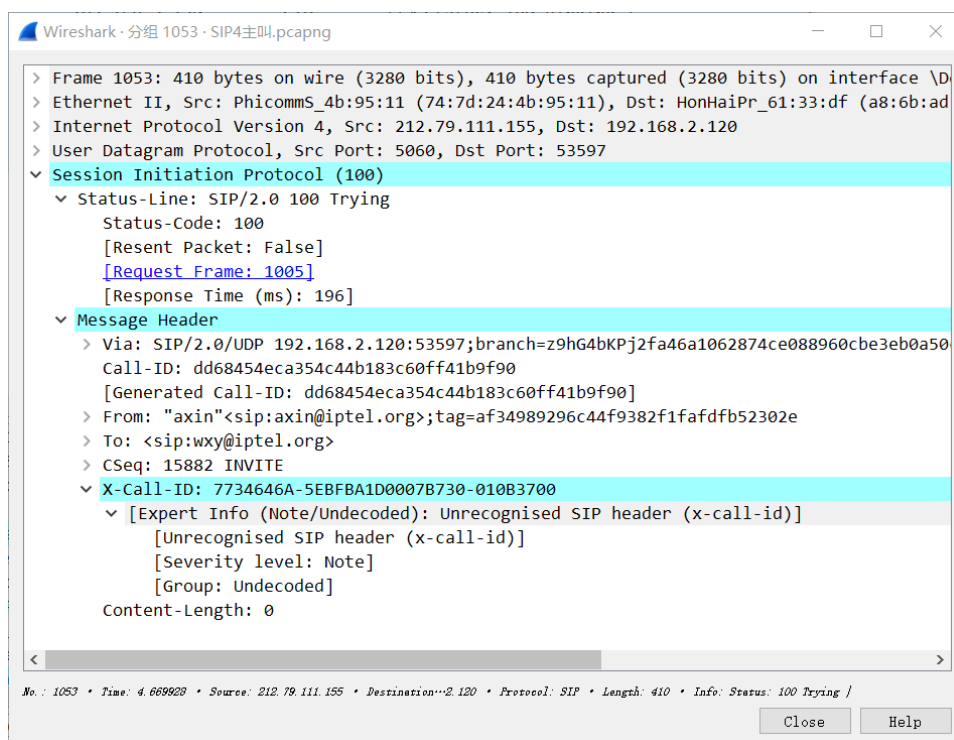
REGISTER 包内容如下：



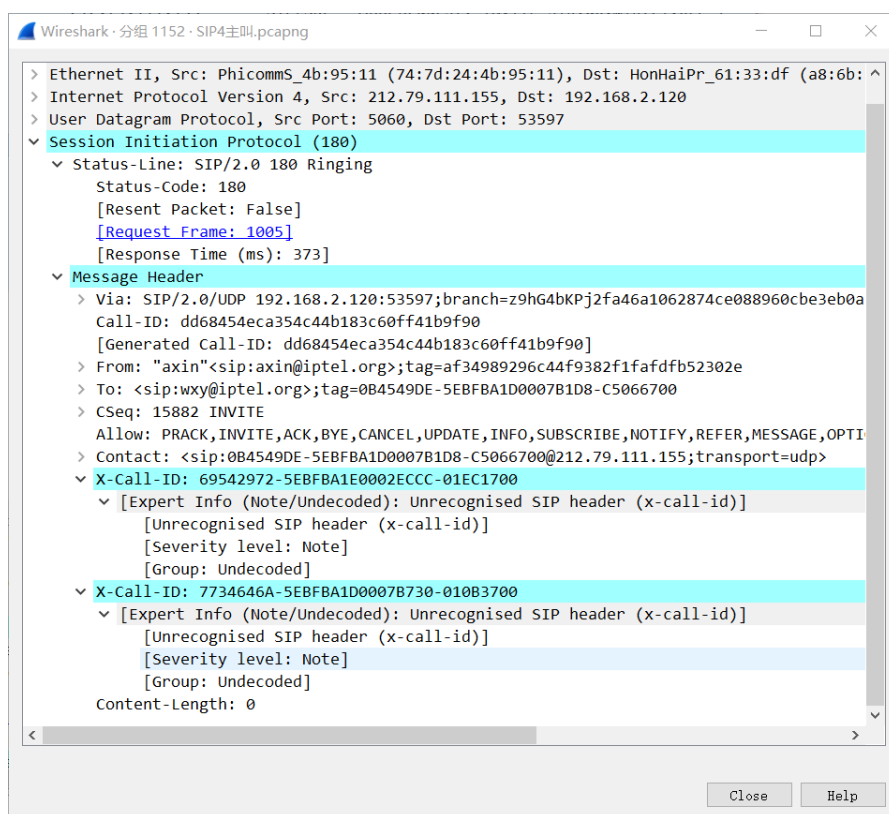
INVITE 包内容如下:



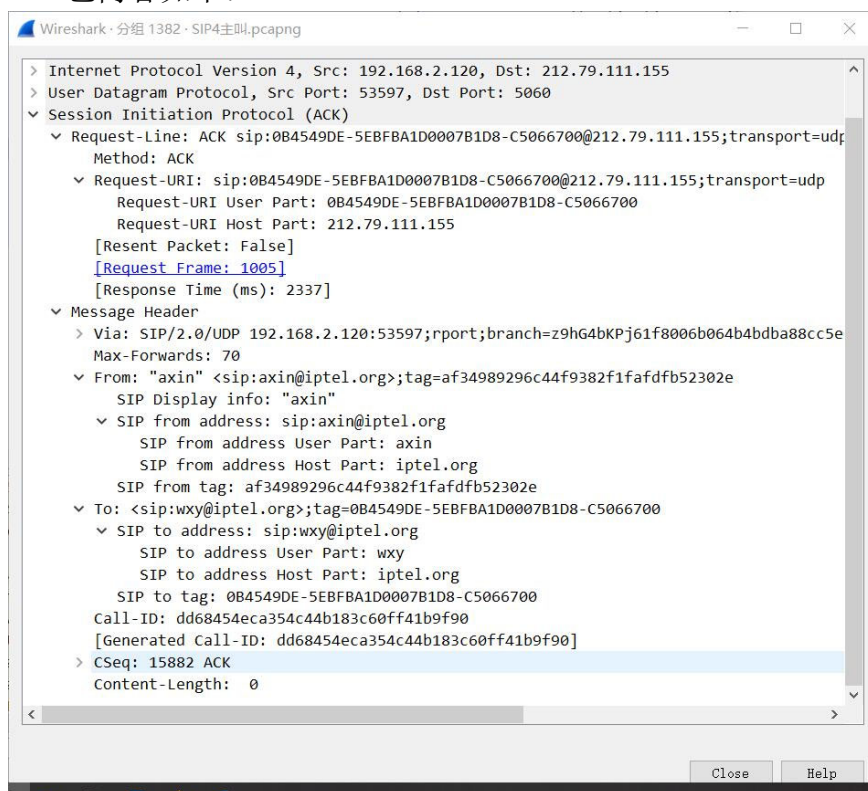
Trying 包内容如下:



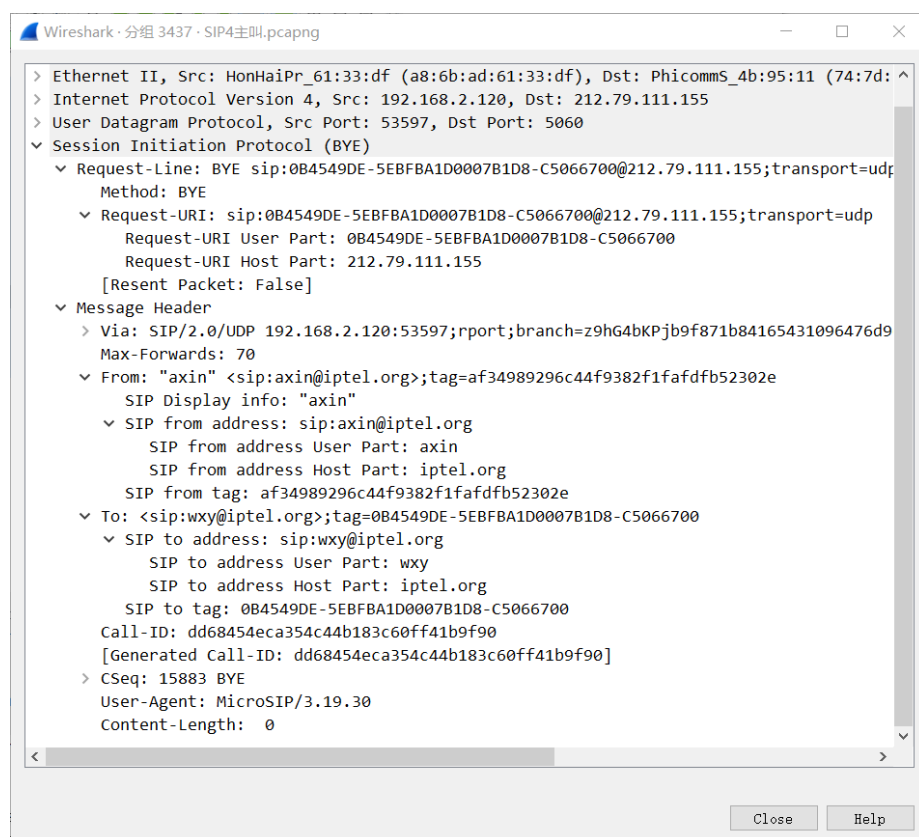
180 Ringing 包内容如下:



ACK 包内容如下:



BYE 包内容如下:



2.5 被叫正在忙碌（可能正在与其他人通话）

可能是因为软件具体实现问题，在被叫正在通话时，对于打入的电话，软件会让用户自己选择是否接通新的通话。无法模拟课件中被叫忙呼叫释放的过程。

因此本组采用自己拨打自己的 SIP 电话，相当于被叫忙的状态。

流程图如下：

被叫忙呼叫释放



- (1) 用户摘机发起一路呼叫，终端代理 A 向该区域代理服务器发起 Invite 请求；
- (2) 代理服务器向被叫终端代理 B 传送 Invite 请求。
- (3) 代理服务器向终端代理 A 发送呼叫处理中的应答信息：100 Trying。
- (4) 终端代理 B 向代理服务器送呼叫处理中的应答信息：100 Trying。
- (5) 呼叫请求送到被叫终端代理 B 后，被叫忙，终端代理 B 向代理服务器送 486 Busy here 被叫忙响应。
- (6) 代理服务器向终端代理 A 转发该响应消息。
- (7) 终端代理 A 向代理服务器回送 ACK 确认消息。
- (8) 代理服务器向终端代理 B 送 ACK 确认信息。

Wireshark 抓包分析：

SIP打自己.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

No.	Time	Source	Destination	Protocol	Length	Info
3173	15.661031	192.168.2.120	212.79.111.155	SIP/SDP	1000	Request: INVITE sip:axin@iptel.org
3219	15.858517	212.79.111.155	192.168.2.120	SIP	364	Status: 100 Trying
3220	15.859972	212.79.111.155	192.168.2.120	SIP	772	Status: 407 Proxy Authentication Required
3221	15.860138	192.168.2.120	212.79.111.155	SIP	404	Request: ACK sip:axin@iptel.org
3222	15.860256	192.168.2.120	212.79.111.155	SIP/SDP	1177	Request: INVITE sip:axin@iptel.org
3276	16.058190	212.79.111.155	192.168.2.120	SIP/SDP	1163	Request: INVITE sip:axin@192.168.1.3:53597;ob
3278	16.067769	192.168.2.120	212.79.111.155	SIP	337	Status: 100 Trying
3279	16.068078	192.168.2.120	212.79.111.155	SIP	377	Status: 486 Busy Here
3306	16.261047	212.79.111.155	192.168.2.120	SIP	363	Request: ACK sip:axin@192.168.1.3:53597;ob
3307	16.262393	212.79.111.155	192.168.2.120	SIP	500	Status: 486 Busy Here
3308	16.262701	192.168.2.120	212.79.111.155	SIP	404	Request: ACK sip:axin@iptel.org
6011	28.381784	192.168.2.120	212.79.111.155	SIP	562	Request: REGISTER sip:iptel.org (1 binding)
6029	28.582335	212.79.111.155	192.168.2.120	SIP	460	Status: 200 OK (1 binding)

当呼叫播出的时候，主叫也是被叫，无法接通电话。具体流程和 ppt 给出的相吻合。

三、实验心得

王兴宇：

在实验的一开始遇到了一些问题，比如我注册的 SIP 账号的服务器 iptel.org 而刘凯鑫注册的是 sip2sip.info，并且我们两个使用的软件也不同，在打 SIP 电话测试时发现，只有他能给我打通，我打他的 SIP 电话提示找不到路径，但是刘兴贤也是注册 iptel.org，我俩就可以正常通话。经过组内讨论，觉得问题可能是出在不同服务器对其他服务器的账号以及软件等的兼容性不是很好，然后刘凯鑫重新注册了 iptel.org 的账号，果然三个人就可以正常互相拨打电话了。

经过这次的 SIP 抓包实验，对不同情况下 SIP 会话的包进行抓包分析，我对 SIP 协议的特点、结构以及 SIP 连接建立和拆除的过程有了深刻的了解，也对 SIP 请求消息的各种情况（INVITE,ACK,BYE 等）和响应消息（100Trying, 200OK 等）有了清晰的认识，也对 SDP 和 RTP/RTCP 有了简单地了解。虽然只是简单地抓包分析实验，但是很有意义，我学到了很多。

刘凯鑫：

本次实验经历了一些挫折，首先是注册 SIP 账号时，由于确认邮件被认为垃圾邮件耗费了一段时间；

但使用的软件操作简单明了，配合 WireShark 抓包分析，整个实验在组内合

作完成的比较顺利。实际操作发现主叫拨打电话之前有一个认证过程，简单分析了 407 Proxy Authentication Required 和对应的 ACK。查阅资料弄清楚了开始几个多出来的包的作用。对于 SIP 网络电话在广度上有所拓宽。主叫方会收到代理服务器发送的 407 Proxy Authentication Required，标志了客户端应当首先在 proxy 上通过认证。这个返回码用于应用程序访问通讯网关(比如，电话网关)，而很少用于被叫方要求认证。

最困难的问题出在被叫无应答的情况，ppt 中给出了两种不同情况：

1 主叫超时未收到 ACK

2 被叫超时无人摘机

本身是很好理解的两种情况，但是在实际的实验中。结果确实两种情况混合在一起。(详见被叫未接听的流程图)。网上查询资料也没有遇到类似情况，和组员反复实验，证明该情况是可复现的。最终咨询老师，分析可能是软件的实现方式不同。虽然和课件中有所不同，但是分析其流程同样是合理的。

刘兴贤：

本次实验通过拨打 SIP 电话与抓包分析，使我更清楚了 SIP 电话的协议流程，与具体实现。

由于本次过程开始，我直接注册了域名为 `iptel.org` 的账号，因此并未遇到组内其它两名同学的跨域名的 SIP 电话打不通的问题。最终，我们组内一致使用了 `iptel.org` 域名的账号。试验得以顺利进行。因此我的实验过程还是相当顺利的，在分析多种情况时，为了体现组内不同成员的参与度，我们采用了三个人的账号交换主被叫探讨不同情况，最终由不同的人分析不同的情况。

实验过程中，我们遇到了相当令人困惑的两次 Invite 中间夹杂了 407 Proxy Authentication 的包，经过多次重复试验，每一次都会出现该包。因此，我们认为这应该是一种普遍情况，因此我们去查询了 SIP 协议的官方文档，最终发现了，这是从 HTTP 协议中借鉴来的鉴权过程，并在情况 2.4 中进行了解释。

令我们骄傲的是，或许其他很多组不会注意到这个鉴权机制，而我们发现后进行了一系列资料查询，最终搞明白了这个问题。因此收获相当大。